


REVISTA DIGITAL
#3

Noviembre 2019

Geopolítica digital
Geopolítica digital y BigTech: Una vuelta de tuerca a la cultura material corporativa

Buenas prácticas
Recomendaciones para nuestra seguridad digital

Ciberseguridad
Ciberseguridad, un desafío para América Latina y el Caribe

Espionaje digital
La muerte de la privacidad que nunca tuvimos

internetciudadana.net

**Revista Digital "Internet Ciudadana"**
**n° 3 – Octubre 2019**

## ÍNDICE



Publicación digital del proceso regional en América Latina y el Caribe hacia un Foro Social de Internet (FSI).

Como foro temático del Foro Social Mundial (FSM), el Foro Social de Internet es una iniciativa popular y abierta, cualquier persona motivada a defender el interés público puede sumarse, el único requisito es adherir a la Carta de principios del FSM y sus principios anti-neoliberales.

Para inscribirse en la lista de correos del proceso de intercambio regional latinoamericano-caribeño, o para enviar colaboraciones a esta publicación pueden escribir a:
fsi-alc@internetciudadana.net

Para más información:
https://al.internetsocialforum.net

## Equipo Editor

Aram Aharonian, Sally Burch, Ariana María López, Isel del Castillo, Eduardo Rojas, Montserrat Boix, Irene León, Javier Tolcachier.

Imagen de tapa: Gentileza de Photo Mix

Diagramación realizada con los software libres Scribus, Inkscape, Gimp

# Editorial

La llamada "red de redes" se ha convertido hoy en un espacio de interacciones indeludible. El fenómeno ha sido funcional a la globalización impulsada desde las corporaciones en su afán de sobrepasar cualquier límite y limitación de soberanías estatales. Nadie puede y nadie quiere quedar afuera, para bien y para mal.

Dejando de lado toda apreciación inocente, la vinculación individual a la red se traslada a una maraña de encadenamientos ocultos a la mirada y el control. Aún más, toda la estructura de internet, apenas comprensible para expertos, es opaca e inasible para quienes a diario se relacionan con y en ella.

En esta esfera multiconectada de la Internet actual cuya dominancia mercantil corporativa amenaza con inhibir cualquier voluntarismo individual, ¿es posible pensar en protección informática o ciberseguridad? ¿Acaso pueden los Estados resistir la presión multinacional, la agresión cibernética, el ataque desdemocratizador de la información manipulada? ¿Cómo abrir brecha a una genuina incidencia colectiva y lograr a la vez protección del espacio personal, habiendo sido degradados a la categoría de masa informacional individualmente identificable? ¿Cómo dejar de ser proveedores incautos de datos, materia prima gratuita que engordará las arcas de las ya principales empresas del planeta?

¿Cómo sostener los sueños de independencia, de soberanía, las aspiraciones de justicia social en este ambiente emponzoñado? ¿Cómo garantizar el acceso irrestricto al conocimiento común, la distribución equitativa de sus frutos, el crecimiento social que Internet prometió alguna vez?

Con esta nueva edición de Internet Ciudadana probablemente no logremos abordar la extensión y complejidad del tema, ni dar certezas definitivas sobre como sobreponernos a la indubitable inseguridad digital y otras materias de índole semejante. Pero si logramos lanzar preguntas certeras e indagar algunas pistas, este número habrá cumplido su misión con creces.

**Equipo editorial**






# Geopolítica digital y BigTech: Una vuelta de tuerca a la cultura material corporativa

por Josué García Veiga

Las transformaciones políticas, económicas y tecnológicas en la última parte del siglo XX dieron lugar a un profundo proceso de re-ordenamiento en la jerarquía de relaciones de poder que articulan el mercado y la hegemonía mundial (Ceceña, 1990). Los cambios se caracterizaron por acelerados procesos de innovación y desarrollo tecnológico (primordialmente en los campos de la microelectrónica, el poder de cómputo, la informática, la programación y la mejora de los materiales, entre otros) que lograron conformar el paradigma tecnológico de lo que comúnmente se denomina Era Digital. Dicho proceso se imbricó (como causa y consecuencia) con cambios institucionales pro-mercado que pusieron fin a un largo periodo de políticas intervencionistas de corte keynesianas (Estado de bienestar, desarrollista e intervencionista).

Actualmente la tecnología digital y su operatividad en redes son el eje de las TICs (tecnologías de la información y comunicación) que han logrado constituirse como una tecnología genérica por el hecho de ser un "sistema que por su amplia aplicabilidad es susceptible de utilizarse en todas las ramas de la producción y en las actividades humanas en general" (Rivera et. al., 2018). Estas tecnologías están posibilitadas por una amplia infraestructura de Internet: banda ancha y dispositivos sensoriales (GPS, cámaras, WiFi, etc.) que se caracterizan por conformar un sofisticado sistema de recopilación de datos en tiempo real (Morozov, 2018). En este sentido, los datos digitales (la información) son "la célula" del funcionamiento de las TICs en su estado actual y el elemento estratégico de la geopolítica digital contemporánea.

Ante la tesis del pensamiento liberal, y apologeta del desarrollo tecnológico que enaltece las promesas del próximo estadio de la era digital como solución general a las problemáticas más acuciantes de nuestra época (estancamiento secular económico, incremento de la polaridad y desigualdad social, cambio

climático, por señalar algunas), contrastamos una lectura de las relaciones de poder y la acumulación de capital de los actores que disputan el dominio de la vanguardia tecnológica digital.

Se observa cómo lo que prometía ser en sus orígenes un proyecto libertario de la comunicación para compartir información al alcance de todas las personas, ha devenido en una concentración del ejercicio del poder, intensa y aparentemente ilimitada en unas cuantas plataformas digitales (Gawer y Cusumano, 2013)[1], o bien, en grandes servidores sirena[2], retomando la metáfora y el término de Lanier (2014). Su entrada en escena se puede rastrear desde inicios del nuevo siglo con los proyectos Web 2.0 –plataformas de trabajo colaborativo– y las inversiones masivas por parte de capitales tecnológicos de Silicon Valley ante la explosión de la crisis dot.com (Burch, 2018). Esta concentración es mayor que el alcance de la descentralización ocasionada por el quiebre del anterior modelo de producción fordista. Recientemente la tendencia de polaridad y disrupción digital (McKinsey, 2015) se ha acrecentado aceleradamente a nivel mundial (inter e intranacionalmente).

## Plataformas digitales: funcionamiento

Hoy en día, independientemente del negocio en el que se especializa cada una de las plataformas digitales, podemos generalizar un modelo de negocio común. La clave recae en su posición privilegiada al interior del sistema digital sensorial de recopilación de datos. En un primer momento suelen ofrecer servicios y/o productos aparentemente gratuitos (o a un costo prácticamente nulo)[3], pero su retribución es la información personal (en gran medida sin consentimiento pleno por parte de los consumidores), la cual es recolectada y almacenada por las plataformas.

En un segundo momento se abre todo un abanico de posibles actividades altamente rentables, que se pueden valorizar una vez concentradas inmensas cantidades de información en los grandes centros de cómputo privados. El big data consiste en capturar, almacenar y analizar las grandes bases de datos; las técnicas de análisis especializadas (analytics, minería de datos) generan nueva información a partir de identificar patrones, relaciones y estimar tendencias en las bases de datos originales, para, posteriormente, ser vendida a terceros agentes privados o públicos con diversos fines: lucrativos, publicitarios, seguridad, espionaje, políticos, entre otros (Google, Facebook, Twitter, YouTube, Tencent).



Una segunda opción es aprovechar la escala de usuarios contenida en sus plataformas para vender el acceso a terceros que busquen relacionarse con los usuarios de diversas formas: productos, publicidad, contratación, etc. (Amazon, Alibaba, Mercado Libre). Una tercera vía es la utilidad de los datos como materia prima del principio de retroalimentación necesario para el desarrollo, perfeccionamiento e innovación de nuevos "algoritmos", esto es, de los métodos mediante los cuales se ordenan una serie de pasos sobre estructuras computacionales para realizar una tarea dada (Terranova, 2018). Estos algoritmos yacen detrás de la mayor parte de innovaciones y ensayos incipientes de nuevas técnicas y tecnologías como el aprendizaje automático (machine learning), el aprendizaje profundo (deep learning), la ciencia de datos (Data Science), las interfaces cerebro-computadora (brain-computer interfaces), por señalar algunas.

## Los datos digitales: recurso estratégico en la hegemonía mundial del siglo XXI

De lo anterior se desprende que la articulación y organización en redes digitales dista de ser un sistema homogéneo, ya que éstas son estructuras altamente asimétricas, con jerarquías entre los nodos que las componen. La principal diferencia radica en su poder de cómputo. Las grandes plataformas digitales controlan un inmenso poder de cómputo para extraer, procesar y analizar datos.[4]

Es así que en el capitalismo "digital" contemporáneo, el poder de cómputo y los datos son recursos estratégicos altamente disputados. El carácter estratégico de los datos ha sido alcanzado debido a las potencias históricas de las fuerzas productivas tecnológicas actuales (digitación-redes). Por lo tanto, aquellos sujetos que logren dominar la extracción, almacenamiento y análisis de datos, accederán no solo al monopolio de grandes flujos de rentas económicas (plusvalía extraordinaria) sino que además estarán en una posición privilegiada (vanguardia tecnológica), lo que les permite una mayor capacidad para controlar los ritmos y formas en las que se desarrollan las nuevas tecnologías (Rivera, et. al. 2018; Morozov, 2018).

Ello también les facilita renovar y garantizar su posición de liderazgo en la vanguardia tecnológica en los nuevos nichos, usos y aplicaciones como el Internet de las cosas, la inteligencia artificial, la conducción autómata, el reconocimiento facial, la realidad aumentada, entre otras, con un amplio rango disruptivo en varias industrias y actividades humanas (transporte, comercio, industria, servicios educativos, salud, turismo, seguridad, espionaje, servicios bancarios, el complejo militar y de armas, actividades de ocio y de entretenimiento, etcétera. Actividades donde sobresalen empresas como Microsoft, Apple, Baidu, Alphabet, Uber, entre otras).

Por ende, no es menor la atribución de "estratégico" que le asignamos a los datos para el estudio y comprensión de la competencia por la vanguardia tecnológica digital y el liderazgo económico mundial del siglo XXI.[5] Desde una visión geopolítica de las plataformas digitales líderes más importantes, encontramos que en su mayoría son desarrolladas por corporaciones transnacionales (CTNs) con sede en Estados Unidos y China. Estas CTNs digitales de frontera son conocidas como BigTech (gigantes tecnológicos), que junto con sus estados se encuentran inmersas en una competencia tecnológica que se puede ilustrar en los acrónimos popularizados por la prensa y textos especializados como: FAANG (Facebook, Amazon, Apple, Netflix y Google) vs BAT (Baidu, Alibaba y Tencent).[6]

Actualmente las BigTech ocupan importantes posiciones entre las empresas más grandes al interior de la economía de Estados Unidos, si bien es cierto que no encabezan el ranking por ventas a nivel mundial –manteniéndose por detrás de las grandes empresas petroleras (Sinopec Group, China National Petroleum, Royal Dutch Shell, BP, Exxon), energéticas (State Grid), automotrices (Toyota, Volkswagen) y aseguradoras (Berkshire Hathaway)–[7] han logrado expandirse aceleradamente en el mundo, principalmente mediante un proceso frenético de fusiones y adquisiciones, que ha servido como palanca para incrementar su emporio económico al subsumir cualquier amenaza naciente, por muy pequeña que sea pero con grandes promesas, como las startups.[8] Lo que tiene como efecto secundario bloquear la competencia, aumentar las barreras a la entrada y generar una estructura de mercado concentrada en conglomerados oligopólicos.

Por otra parte datos del Wall Street Journal (2019) revelan que las BigTech son actualmente las corporaciones más valiosas del mundo según su capitalización bursátil, con Amazon al frente seguida de Microsoft, Alphabet y Apple.[9]

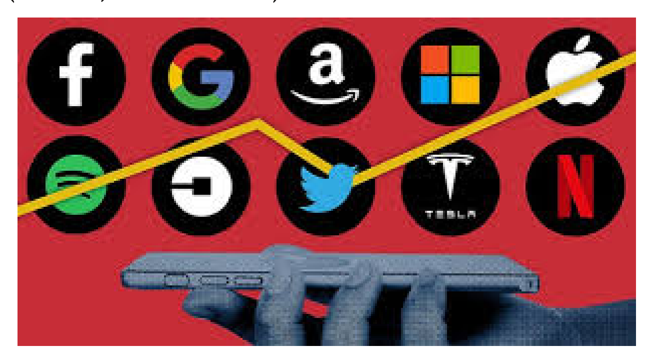
## Delineando el poder de las Corporaciones BigTech

Estudiar el poder de las BigTech no debe reducirse únicamente a los indicadores cuantitativos sobre su habilidad para acumular cuantiosas rentas económicas. La Corporación Transnacional es un grupo de poder (Ceceña, 2016:108) que yace en la cima del estadio actual del capitalismo con capacidad de acción que va más allá del plano de lo "económico" (extracción, transformación, circulación y distribución). Su rango de influencia trasciende las fronteras de los estados-nación (Ornelas, 2016 y 2017), moldeando la articulación de los circuitos que reproducen el sistema-mundo capitalista para generar un "modo de vida" (Ceceña, 2017:8).

La realización de sus actividades ordenadas bajo la búsqueda insaciable de ganancias y poder, conllevan una huella que no solo es ecológica (material-energética) sino también simbólica (Ceceña, 2017). Las CTNs definen de manera sustancial las tendencias civilizatorias contemporáneas al instalar "forma[s] de ser y estar en el mundo", moldear los modos de pensar junto con los deseos, los sentidos, las prácticas sociales y la construcción de identidades e imaginarios colectivos (Inclán, 2018).

Desde este panóptico se vislumbra que las grandes plataformas digitales, como forma particular de CTNs, llevan al límite la forma civilizatoria capitalista como nunca antes se había visto. Los servidores sirena (FAANG, BAT y otros) se han convertido en la tecnología por excelencia de difusión, transmisión e instalación de lo que Inclán (2018) denomina "cultura –material– corporativa".

Los vectores estatales específicos (Ornelas, 2017) en los que el Estado se relaciona con estas corporaciones hace necesario que contemplemos el marco socio-institucional dentro de nuestra investigación para determinar la forma real en la que se "regula" el desarrollo de la tecnología digital, el reparto de sus riquezas y potencialidades entre la sociedad (Rivera, et. al. 2018).[10]




Las plataformas digitales son, en mayor medida, la principal (no la única) interacción con el mundo, tendencia que se observa con mayor claridad en las grandes urbes. Son estas CTNs BigTech la nueva infraestructura de poder donde la voz mántrica del espíritu empresarial hace eco con todo su esplendor en todos los rincones de la vida moderna.[11] El comportamiento general (nunca absoluto) de las plataformas digitales ha servido para promover e impulsar la creatividad individual en aras de expandir el reino de las mercancías, el e-commerce (Amazon, Alibaba, Airbnb y otros) más allá de la ficción ha creado un mercado "virtual" que nunca descansa, al que se puede acceder desde cualquier geografía para ofrecer y demandar una inmensa variedad inimaginable de productos y servicios a lo ancho del mundo y todo bajo un solo slogan: "¡Todo(s) tiene(n) un precio!". Con la misma variedad encontramos una gran cantidad de plataformas de autoempleo (Uber, Handy, Upwork, and PeoplePerHour, IKEA, TaskRabbit, Deliveroo, UberEats, Foodora, etc.), léase autoexplotación (exploitation by yourself), que surgen a partir de la filosofía de la flexibilidad polivalente multi-task consolidándose como un nuevo tipo de economía, llamada de "concierto" o "colaborativa" (gig economy)[12].

En este tipo de prácticas toda persona presume del privilegio de ser su propio jefe, pero olvidan que sus "libertades" se ven mermadas por la precariedad laboral (al no contar con la mínima protección social de gastos médicos, pensión, fondo de retiro o de otro tipo similares) y los

bajos salarios, que son resultado de la presión mercantil por abaratar al mínimo la mano de obra, lo que lo obliga a tener mayores "estímulos" para reducir su "tiempo libre" e ingresar por su "propio deseo" a la competencia intensificada.

Las BigTech están dando una vuelta de tuerca a la "cultura corporativa" en la sociedad y con ello la interiorización e impersonalización del poder en el capitalismo del siglo XXI (Inclán,



2018). Empujan con fuerza lo que podría tratarse de un nuevo ciclo de capital vigoroso, pero al mismo tiempo se exacerban sus tendencias seculares de concentración, explotación, dominación, despojo y dependencia tecnológica centro-periferia.

Por si fuera poco, este nuevo tipo de patrón de sí mismo debe sujetarse a una evaluación constante respecto a una norma de "buen comportamiento" (sea de vestimenta, lenguaje "sugerido", etc.). Por otra parte, frente al alto grado de atomización alcanzado por la sociedad actual, están las plataformas conocidas como redes sociales digitales (Facebook, Twitter, Tencent, etc.) que cumplen con la función de crear "artificialmente la imagen de una gran comunidad". En estas redes la búsqueda de vínculos con otras personas mediante algún tipo de nexo común (intereses, gustos y otros), termina tendencialmente sometida por la constante penetración "selectiva y personalizada" (gracias a la vigilancia permanente) de contenidos simbólicos. Estos contenidos terminan por influenciar en la concepción de vida de los usuarios, en sus prácticas de lenguaje y comunicación, de comer, de vestir y hasta en la determinación de su "libre" votación en elecciones políticas.

*(*) Josué García Veiga es Maestrante en el Posgrado de Estudios Latinoamericanos de la UNAM-México. Licenciado en Economía y miembro del Laboratorio de Estudios sobre Empresas Transnacionales perteneciente al Observatorio Latinoamericano de Geopolítica-UNAM-México.*

*Contacto: josuegave@hotmail.com*

## Notas

1 "Una plataforma digital constituye una red articulada en torno a un eje que puede ser tecnológico [Apple, Alphabet, Baidu], comercial [Amazon, Alibaba] y social [Facebook, Tencent], posibilitando así la integración y la acción coordinada de multitud de agentes que gravitan en torno al eje

de la plataforma, formando un ecosistema y posibilitando la superación de las fronteras entre mercados" (Rivera, et. al. 2018).

2 Los servidores sirena son "recursos de computación cuya potencia supera a la de todos los demás nodos de la red y que, en un principio, parece asegurar a sus dueños el camino hacia un éxito garantizado e ilimitado. Pero los beneficios son ilusorios y no tardan mucho en conducir a un gran fracaso" (Lanier, 2014).

3 Este modelo de negocios gratuito (modelo freemium) hoy en día no es condición necesaria. Actualmente han emergido plataformas digitales que cobran mediante suscripciones o comisiones por los diversos servicios y productos ofrecidos (ejemplos: Spotify Premium, Netflix, entre otras). Algunos autores como Morozov (2018) estiman que en los próximos años aumente la privatización del viejo modelo freemium debido a las nacientes regulaciones que podrían reducir la rentabilidad junto con las presiones por parte de los fondos de riesgo (venture capital) que abundan en el financiamiento de startups exigiendo altas rentabilidades.

4 En toda comunicación "[…] a través de una red de ordenadores […] quien disponga del ordenador más potente se hará con la superioridad informacional" (Lanier, 2013). Más adelante agrega que "[…] tener poder significa poseer la superioridad informacional, obtenida mediante el control del ordenador más efectivo de una red".

5 La apreciación estratégica de los datos digitales no se limita al periodo naciente del Internet y de la consolidación de las plataformas digitales, sino también en las tendencias tecnológicas del futuro más cercano, para lo cual citamos a Lanier: "la razón por la que es probable que el valor de los datos personales aumente es que son la materia prima de los sistemas automatizados o hipereficientes, y estos serán cada vez más numerosos" (2013).

6 Aunque pareciera que la asignación de acrónimos y su uso es indistinto, tales como GAFAM (Google, Amazon, Facebook, Apple y Microsoft) o FANG (sin Apple o con más empresas) cuya invención se atribuye a Jim Cramer, comentarista financiero de CNBC (Brodie, 2013); de fondo, los sujetos desdoblados en disputa no cambian: Estados Unidos sus empresas vs China y sus empresas.

7 De acuerdo con el listado de Fortune Global 500 para 2018 Apple ocupa la posición 11 con ingresos de 229 miles de millones de dólares (mmd), Amazon posición 18 con 177 mmd, Alphabet posición 52 con 110 mmd, Facebook posición 274 con 40 mmd, Alibaba posición 300 con 37 mmd, Tencent posición 331 con 35 mmd (véase listado de Fortune Global 500 disponible en http://fortune.com/global500/).

8 Algunos ejemplos de fusiones y adquisiciones (F&A) importantes en la industria tech son los casos de Facebook cuando compró a Instagram en 2012 y poco tiempo después a WhatsApp en 2014; por su parte Alphabet ha invertido en 300 startups desde 2013 y Amazon adquirió a Whole Foods Market en 2017. Las F&A se han acelerado en la rama de Inteligencia artificial en todo el mundo desde 2010 (The Economist, 2017).

9 A principios de enero de 2019 Amazon se ha convertido en la corporación más valiosa del mundo con un valor de 797 mil millones de dólares (mmd), seguida de Microsoft con 783 mmd, Alphabet (Google) con 756 mmd y Apple de 700 mmd (Zweig, 2019).

10 Las CTNs estadounidenses y chinas se vinculan con los estados-nación de manera diferente. Una estrategia de Alibaba (líder chino en el comercio electrónico) para entrar en mercados latinoamericanos ha sido buscar acuerdos con los gobiernos locales. Este fue el caso de la firma de acuerdos por Dilma Rousseff en 2014 para el caso de Brasil (Xinzhu, 2014) y Enrique Peña Nieto en 2017 para México (Reuters, 2017).

11 La difusión, transmisión e instalación de la cultura corporativa y el espíritu empresarial se ven facilitados mediante las múltiples combinaciones posibles de hardware y software que constituyen las diferentes plataformas digitales existentes pero que principalmente están diseñadas para el consumo de contenidos y formas disminuyendo cualquier oportunidad para generar nuevos contenidos. Lanier (2014) pone el ejemplo de los celulares y las tabletas en el sentido de que sirven únicamente para descargar, ejecutar y consumir aplicaciones que han sido "aprobadas" (en su mayoría propiedad de grandes plataformas digitales). La diferencia respecto la vieja computadora personal (PC) es que en ellas todavía existe un grado de libertad para ordenar y programar en tu elección y gusto, y en los otros dispositivos estás limitado prácticamente a consumir lo que ofrecen las empresas.

12 La gig economy es el nombre común del tipo de mercados en-línea para trabajos en el corto plazo y de auto-empelo (freelance). Existen desde el alquiler de domicilios, servicios empresariales hasta los servicios del aseo doméstico (The Economist. 2018).

## Fuentes bibliográficas y/o hemerográficas


Brodie, L. [2013], "Cramer: Does Your Portfolio Have FANGs?", CNBC, https://www.cnbc.com/id/100436754

Burch, Sally [2018], "Redes sociales digitales: un gran negocio", América Latina en movimiento. Redes sociales digitales: enredos y desenredos, Quito, octubre 538, pp. 5-8. Disponible en: https://www.alainet.org/sites/default/files/alem536.pdf

Ceceña, Ana Esther [1990], "Sobre las diferentes modalidades de internacionalización del capital", Problemas del Desarrollo, núm. 81:15-40.

_____, [2016], "La territorialidad de las corporaciones", Ana Esther Ceceña y Raúl Ornelas (coord.), Las corporaciones y la economía mundo. El capitalismo monopolista y la economía mexicana en retrospectiva, Ciudad de México: Siglo XXI-UNAM-IIEc, UNAM-Facultad de Economía, pp. 108-133.

_____, [2017], "Chevron: la territorialidad capitalista en el límite", Ana Esther Ceceña y Raúl Ornelas (coord.), Chevron: paradigma de la catástrofe civilizatoria, Ciudad de México: Siglo XXI-UNAM-IIEc, pp.7-52.

CNN [2018], "Conductores de empresas como Uber y Cabify en Colombia podrían perder su licencia hasta por 25 años", CNN Español, 14 de diciembre, https://cnnespanol.cnn.com/2018/12/14/conductores-de-empresas-como-uber-y-cabify-en-colombia-podrian-perder-su-licencia-hasta-por-25-anos/

El Tiempo [2013], "Conozca Uber, la aplicación móvil para solicitar taxis VIP", El Tiempo, 30 de Octubre, https://www.eltiempo.com/archivo/documento/CMS-13151160

Fortune [2018], Fortune Global 500, disponible en http://fortune.com/global500/

Gawer, A. y Cusumano, M. [2013], "Industrial Platforms and Ecosystem Innovation", The Journal of Product Innovation Management, pp. 417-433.

Inclán, Daniel [2018], “La otra cara del poder corporativo: tendencias civilizatorias y cultura material”, BoLETín, núm. 6, pp. 48-62, disponible en: http://let.iiec.unam.mx/sites/let.iiec.unam.mx/files/Boletin6Impreso.pdf

Jaimovich, D. [2018], “Cuáles son los países de América Latina con mejor y peor conexión a internet”, INFOBAE, 18 de febrero, https://www.infobae.com/america/tecno/2018/02/18/cuales-son-los-paises-de-america-latina-con-mejor-y-peor-conexion-a-internet/

Lanier, J. [2014], ¿Quién controla el futuro?, Madrid: Debate.
Lara, P. [2018], “Sigue la desigualdad de banda ancha en AL”, Silicon Week, 30 de mayo, https://www.siliconweek.com/mobility/sigue-la-desigualdad-banda-ancha-al-96716

McKinsey Global Institute [2015], Playing to Win. The New Global Competition for Corporate Profits, septiembre.
Morozov, Evgeny [2018], “Introducción”, Capitalismo Big Tech.

¿Walfare o neofeudalismo digital?, Madrid, Enclave, pp. 13-38.
Ornelas, Raúl [2016], “La competencia entre las corporaciones gigantes después de la crisis de 2008”, Ana Esther Ceceña y Raúl Ornelas (coord.), Las corporaciones y la economía mundo. El capitalismo monopolista y la economía mexicana en retrospectiva, Ciudad de México: Siglo XXI: UNAM-Instituto de Investigaciones Económicas, UNAM-Facultad de Economía, 50-107.
_____ [2017], “Hacia una economía política de la competencia. La empresa transnacional”, Revista Problemas del Desarrollo, vol. 189, núm. 48, pp.9-32.
Reuters [2017], “Gobierno mexicano firma acuerdo con Alibaba para permitir a empresas locales entrar a mercado chino”, Reuters, 6 de septiembre, https://lta.reuters.com/articulo/comercio-mexico-alibaba-idLTAKCN1BH2BW-OUSLD

Rivera, M., Lujano, B., García, J. [2018], “El Quinto Kondratiev Global. Bajo desempeño económico, inestabilidad y monopolización en la era digital”, http://marivera-rios.com/articulos/El_Quinto_Kondratiev_Global_2018.pdf
Terranova, Tiziana [2018], “Marx en tiempos de algoritmos”, Nueva Sociedad. Democracia y política en América Latina, n.º 277, septiembre-octubre. http://nuso.org/articulo/marx-en-tiempos-de-algoritmos/

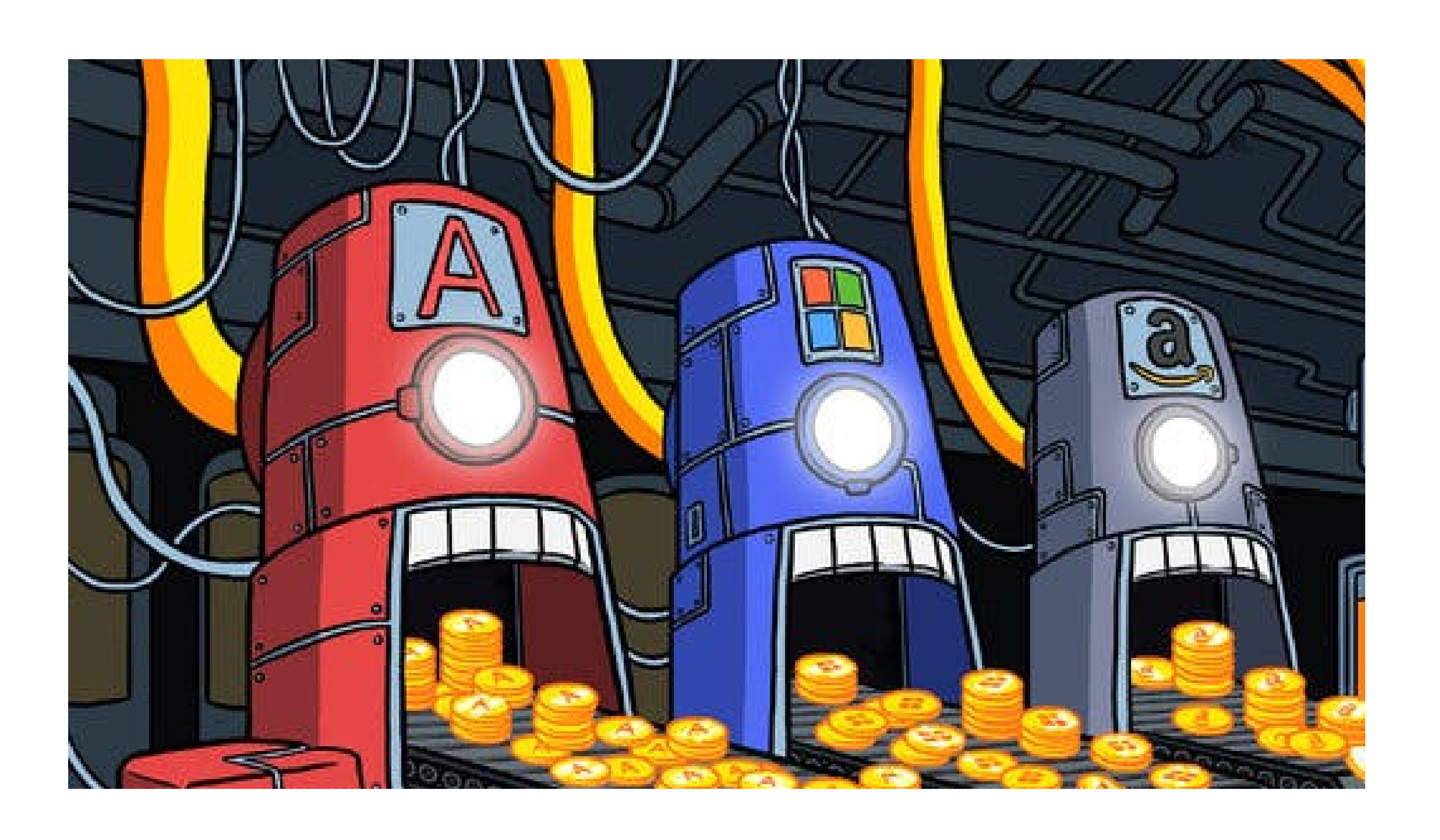
The Economist [2017], "Coding competition. The battle in AI. Artificial intelligence looks tailor-made for incumbent tech giants. Is that a worry?", The Economist, London, 7 de diciembre, https://www.economist.com/news/leaders/21732111-artificial-intelligence-...

_____ [2018a], "Serfs up. Worries about the rise of the gig economy are mostly overblown. But it poses a challenge for tax and benefit systems", The Economist, London, 4 de octubre, https://www.economist.com/finance-and-economics/2018/10/06/worries-about...

Wikipedia [2019], “Anexo: Áreas metropolitanas más pobladas de América Latina”, Wikipedia, https://es.wikipedia.org/wiki/Anexo:%C3%81reas_metropolitanas_m%C3%A1s_pobladas_de_Am%C3%A9rica_Latina

Xinzhu, A. [2014], “Alibaba entra en Brasil”, China Hoy, 26 de septiembre, http://spanish.chinatoday.com.cn/eco/clae/content/2014-09/26/content_642172.htm

Zweig, J. [2019], “What Amazon’s Rise to No. 1 Says About the Stock Market”, The Wall Street Journal, 11 de enero, https://www.wsj.com/articles/what-amazons-rise-to-no-1-says-about-the-stock-market-11547226248



# Algunas recomendaciones para nuestra seguridad digital

Por Comuna Digital

La seguridad digital es, sin duda, una cuestión tan necesaria como vasta e inabarcable. Nunca gozaremos de una seguridad total, pero sí podemos incrementarla considerablemente tomando algunas decisiones. He aquí una breve lista de gestos puntuales o cotidianos que podemos recomendar para reconquistar poco a poco la privacidad que, por el alto valor que tiene, nos están robando. Cada persona podrá encontrar las que mejor le vayan según sus circunstancias. Las medidas que aquí proponemos atienden a amenazas que sufrimos tanto a nivel personal como colectivo.

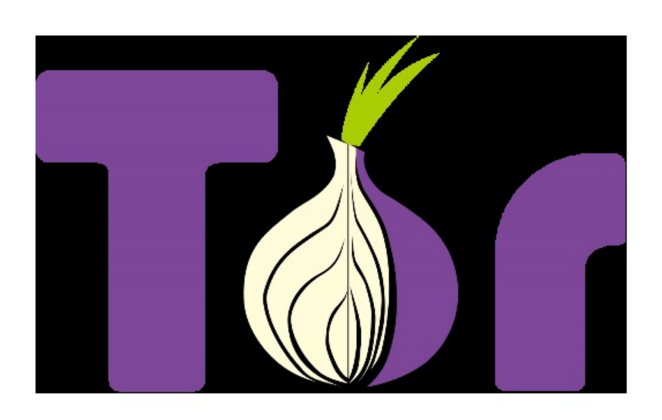
**Ojo con los datos que exponemos**

A veces, para usar un servicio o descargar algo nos piden algún dato personal (dirección de correo, número de teléfono, etc.) que, aparentemente, no tiene relevancia para lo que queremos hacer. Lo más probable es que se use para identificar nuestro perfil y añadirnos a una base de datos. A partir de ella, podremos recibir publicidad no deseada, ser objeto de seguimiento o sufrir algún tipo de ataque. Cuantos menos datos demos sobre nosotros, mejor.

**Usar preferentemente herramientas que no vivan de nuestros datos**

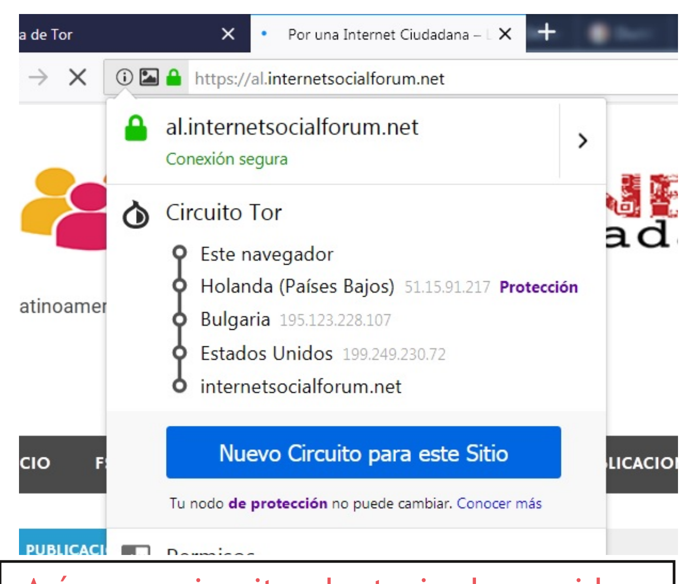
Si una entidad pide más datos de los necesarios para proporcionar su servicio, podemos presuponer que va a comerciar con ellos, vendiéndolos a gobiernos y a otras empresas. En esta línea, nos puede convenir optar por los servicios que no requieran nuestros datos personales, que acepten que seamos anónimos. Es una forma de transitar juntos hacia un modelo en el que podamos comunicarnos tranquilamente sin estar bajo vigilancia continua. Viven de vender nuestra información los servicios de multinacionales como Google —dueña de YouTube—, Facebook —que posee Instagram, Whatsapp y Messenger—, Microsoft, Amazon o Yahoo, entre otros. Se financian de otra forma, sin recurrir a la venta de datos personales, las comunidades de Disroot, RiseUp, Matrix, Autistici/Inventati, Framasoft, Diaspora, Friendica, Mastodon y muchas más.

Así, por ejemplo, para navegar, en vez de Google Chrome, puedes usar FireFox o, incluso mejor, IceCat, que es una derivación de FireFox optimizada de cara a la privacidad. También te puede interesar navegar con Tor.



**Tor**

Es un sistema muy peculiar para navegar por internet de manera anónima. Nos conectamos mediante el navegador correspondiente según el sistema operativo que estemos usando.

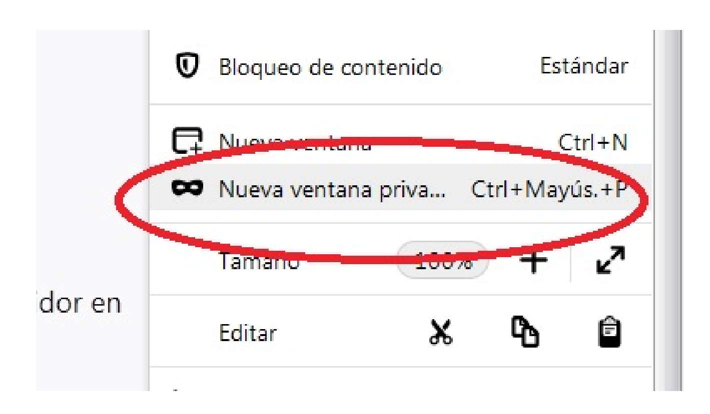



Así es un circuito aleatorio de servidores cuando navegamos con Tor.

Entonces, nuestro navegador, en lugar de consultar el sitio que queramos ver, se conectará a otro servidor intermedio, este a otro, y ese a un tercero. Finalmente, el tercer servidor consulta el sitio que queremos visitar. Puesto que la información circula cifrada a través de varios servidores aleatorios (ver ilustración), situados en cualquier parte del mundo y que actúan como capas de anonimato, es prácticamente imposible —aunque nunca al cien por cien— que alguien deduzca que quien está realmente consultando el sitio eres tú. Aquí lo puedes ver más claro.

**Navegar en modo incógnito o privado**

Esto sirve para no dejar rastros de nuestra actividad en el dispositivo que estamos usando. La opción suele estar visible desplegando el menú principal de tu navegador. Es especialmente útil en dispositivos compartidos con otras personas —ya sea en un cibercafé, en una biblioteca, en una oficina... o en casa—.




Podría ser comprometedor que la persona que usase el mismo dispositivo que yo encontrase en él ciertos datos de mi historial de navegación o algunos identificadores para iniciar sesión en plataformas. Dicho esto, navegar en modo incógnito no te hace invisible en la red; tus datos circularán y serán captados igual. Su "discreción" se limita a la máquina que uses.

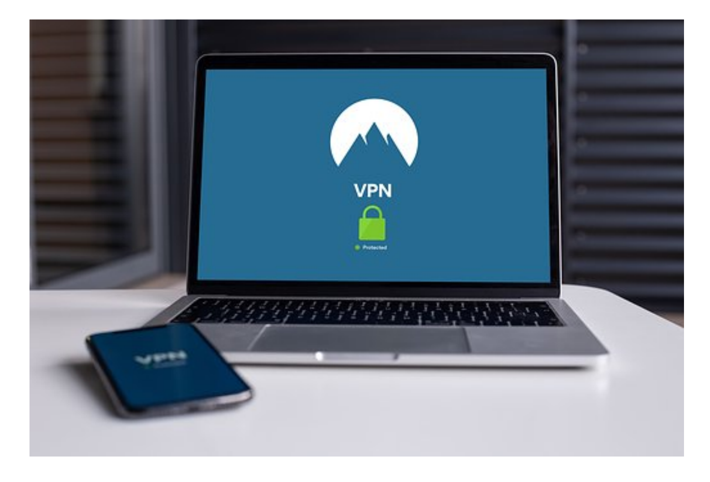
**Cifrado**

Un sistema de cifrado traduce la información que tengamos almacenada o que enviemos —ya sean fotos, mensajes...— a un lenguaje incomprensible para el ser humano, que únicamente podrá descifrar otra máquina que tenga la autorización correspondiente.

Existen varios tipos de cifrado: de transporte, de almacenamiento... Al elegir un servicio de comunicación —como un chat—, conviene optar por aquel que ofrezca cifrado de punto a punto o de extremo a extremo —a veces se lo abrevia como "E2E", del inglés "end to end"—. Este es el que garantiza que al contenido de un mensaje solamente pueden acceder su remitente y su receptor, y nadie más que se encuentre en la ruta de envío.

**Usar una VPN**

Una red privada virtual —Virtual Private Network, en inglés— oculta la IP de tu dispositivo, de manera que navegarás a través de una especie de túnel secreto, siendo muy difícil que te identifiquen. Desde fuera, se verá simplemente una VPN consultando un sitio web, por ejemplo. Es sencillísimo de instalar y usar. Buscando en la web podrás encontrar consejos para elegir una y advertencias sobre sus limitaciones.




**Contraseñas**

No uses la misma contraseña en todas partes. Evita las contraseñas demasiado sencillas —fechas de nacimiento, números de teléfono...— o aquellas que respondan a un patrón más o menos predecible —como frases que tengan sentido—. Las mejores son las que no tienen ninguna lógica aparente.

**Usar más los métodos no digitales**

Podemos replantearnos si tenemos que vincular necesariamente a medios digitales e internet todas esas pequeñas actividades y gestos que componen nuestro día a día digital actual. De esta forma, se verán reducidos algunos problemas como nuestra exposición a las ávidas miradas de terceros, el rastro de información personal que vamos dejando por el mundo digital y nuestra dependencia de la electrónica, además de nuestra huella ecológica o la cantidad de trabajo y dinero que invertimos al año en mantener nuestra vida digital.

**Compartir consejos y trucos como estos en nuestro entorno**

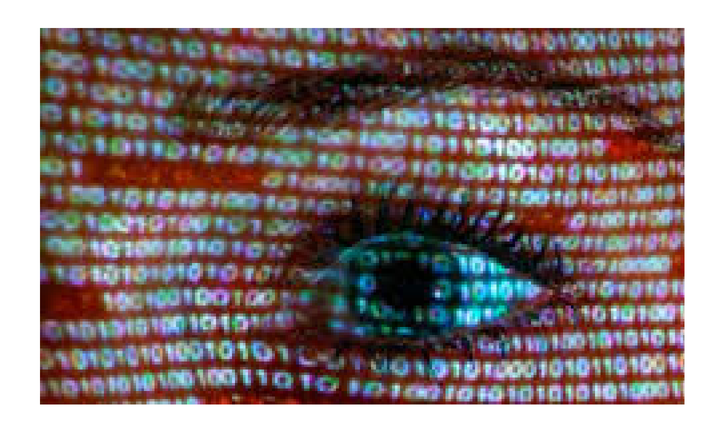
Las mejores formas de protegernos  suele ser actuar en colectivo —la historia de las especies está llena de ejemplos—, y para ello hay que empezar por poner estos temas sobre la mesa. Es una forma de cuidar la comunidad y, sobre todo, es necesario, ya que mi privacidad depende de tus prácticas, y viceversa. Para romper con la dinámica actual, alguien tiene que dar el primer paso, ¿no? ¿Por qué no yo?

## La muerte de la privacidad que nunca tuvimos

por Fernando Buen Abad Domínguez

Los patrones no respetan “privacidades”. No se trata de una “novedad” de ocasión ni de un “descubrimiento” de temporada… el espionaje es manía añeja que se cultiva desde que existe la dominación de una clase sobre otras.

En sociedades divididas en clases no hay poder que sobreviva si no puede saber qué piensa, qué hace o qué planean sus esclavos. En la Historia que conocemos, hasta hoy, no ha habido “poder” que subsistiera sin el uso extorsivo y represivo de toda información sobre quiénes son sus sepultureros y en qué fechas planean sus exequias.



Esa información es vital y, por eso, se hace lo indecible para conseguirla, atesorarla y usarla como arma de guerra económica, ideológica y política. No hay miramientos ni con los “secretos bancarios”. No es lo mismo espiar que expiar.

Sea por la vía de la tortura, sea por la del “confesionario” o sea por la vía de los “estudios de mercado”… los “poderes” hegemónicos han ejercitado siempre el espionaje y el saqueo de la información sobre la vida de personas y organizaciones, como estrategia de “inteligencia” para hacer sobrevivir todas las argucias de la explotación y el hurto de recursos naturales o de materia prima. Lo que comes y lo que defecas, lo que hablas y lo que silencias, lo que anhelas y lo que ni te importa… todo es susceptible de espionaje cuando se quiere a las personas sometidas a caprichos y necesidades de la clase dominante.

Especialmente cuando de lo que se trata es de que trabajemos, hasta deslomarnos, para que ellos vivan como reyes. Cada dato que proveemos al clero, al Estado, a las empresas… es “maná” para las tropelías esclavistas. Fechas de nacimiento, años en las escuelas, preferencias culinarias, monto de los ingresos y de los egresos… caldo potente con información esclavizante. ¿Te gusta cómo se vive?, ¿Qué propones?, ¿De qué dispones? ¿A qué te opones?… Cueste lo que cueste habrá siempre jaurías hambrientas de esa información “inocente” que uno produce.

Como en las “redes sociales”. Detrás hay grandes negocios y el capitalismo, que se convirtió en maestro del espionaje en tiempo real, puso a uno de sus sirvientes mayores a

dirigir la causa negra del espionaje desde la Casa Blanca. Sonría "nos están filmando". ¿Es esa una novedad?

De nada sirve espiar si donde se saquea información no se planta un dispositivo de guerra que mejore el espionaje, siembre confusiones, descarrile las conductas y mejore la rentabilidad de los negocios. Todo junto o en partes. El capitalismo aprendió, rapidito, que "conseguir información" de nada sirve si no se tienen los mecanismos para ponerla a trabajar al servicio de las mercancías y para resolver los problemas de sus crisis de sobre-producción.

No se trata de espiar por el espionaje mismo, se trata de espiar para comerciar, por todos los medios y los modos, habidos y por haber, sean estos faranduleros o bélicos. Hay que desocupar las bodegas y habilitar mercados, cueste lo que cueste. Total, lo pagarán los pueblos. Claro que se espía a todo aquel que constituya "amenaza al sistema", se espía a los revoltosos, a los revolucionarios y a los "terroristas"... se espía a los anarquistas, a los marxistas y a los "troskos"... ya lo sabemos, lo hemos sabido siempre.

También se espía a la "competencia", al que impide fijar precios, al que no deja avanzar la vorágine monopólica del capitalismo y al que se mete con los bancos. Se espía al que atenta contra la "propiedad privada" burguesa y no importa si es la esposa, si es un compañero de oficina, un rector de una universidad, un funcionario público, un cura o es un consorcio trasnacional. Yo te espío, tu me espías, él nos espía... pero ahí donde el burgués invierte dinerito en espionajes, ahí el burgués siembra "pruebas falsas", siembra la firma de su intromisión con dispositivos de espionaje "reloaded".

Ya podrán poner cara de compungidos, de arrepentidos o de indiferentes. Podrán poner denuncias y quejas en organismos nacionales e internacionales. Podrán crear movimientos sociales, y ONG´S de tutti fruti, con la moralina diplomática edificante de gobiernos ofendidos por el espionaje... ya podrán decir misas y podrán redactar enciclopedias; podrán fundar cátedras y alquilar intelectuales reaccionarios que repasen las leyes de Roma y las del Capitolio... fundarán partidos políticos y sectas, endiosarán demonios y satanizarán arcángeles... y mientras, seguirán espiándose los unos a los otros, de arriba abajo, entre "poderosos" y contra los débiles. Espiarán y espiarán porque es parte de su ser y de su "negocio". No van a engañarnos.

El espionaje no es un problema "moral" o un problema de "ética". Es un problema político y táctico que debemos estudiar y desmontar porque se lo usa como arma contra los pueblos y como mecanismo represivo, sofisticado, de control y de sojuzgamiento. Todos sabemos muy bien qué quieren ellos saber sobre nosotros... nosotros sabemos muy bien qué no queremos que ellos sepan, cuando se pone en riesgo la integridad de la lucha y la de los compañeros. No es posca cosa. No luchamos (sólo) contra el espionaje luchamos contra el sistema todo. Una buena parte de la defensa contra el espionaje (y el sistema) de ellos, es nuestra capacidad creativa y nuestras capacidades comunicativas. Shhh... que no se sepa.





# Ciberseguridad, un desafío para América Latina y el Caribe

Por Arantxa Tirado, Silvina Romano, Tamara Lajtman y Aníbal García Fernández / CELAG

Desde hace al menos una década, los temas relacionados con la seguridad informática o en las redes sociales están acaparando mayores espacios en la prensa, reflejo de su mayor presencia en la vida cotidiana y, también, en la política. América Latina y el Caribe (ALC) no escapa a esta lógica. A pesar de no ser un área especialmente preocupada por el tema, como lo demuestra que la mayoría de países del área no tengan una estrategia de ciberseguridad,[1] la región se ve como un ámbito de expansión. El Banco Interamericano de Desarrollo (BID), de hecho, considera a la región una zona vulnerable y calcula en 90 mil millones de dólares el costo del cibercrimen para ALC.[2]

## ¿Qué es la ciberseguridad?

Por ciberseguridad se entiende la "capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información"[3] frente a ciberataques que abarcan potenciales delitos como: difusión de virus, espionaje online, robo de datos o información confidencial de empresas e individuos, manipulación en redes sociales, difusión de noticias falsas o ataque a sistemas informáticos de países enemigos para inhabilitar áreas estratégicas, como algunos sostienen que pudo suceder durante los apagones de marzo de 2019 en Venezuela.[4]

## Ciberseguridad y mercado en América Latina

La consultora Return Comstor espera que en 2019 el mercado de la ciberseguridad latinoamericano alcance los 12 billones de dólares. La región es el cuarto mercado más grande de telefonía móvil y más de la mitad de su población usa internet. Fortinet es una de las empresas líderes en proveer servicios de protección por internet. Tan sólo en Perú abarca poco más del 60% de dispositivos protegidos por sus servicios. Le siguen Brasil, Colombia, Chile, México, Venezuela y Argentina.[5]

Las empresas israelíes también son grandes proveedoras de servicios en la región. Verint y Elbit son los proveedores de servicios de ciberseguridad más destacados y, en el caso particular de México, la introducción de software de este tipo ha sido utilizado por el Gobierno de Enrique Peña Nieto para espiar a periodistas y opositores.[6]

Uno de los clientes privilegiados de la ciberseguridad israelí es Brasil, mercado que comparte con Estados Unidos (EE. UU.), y que está en vistas de expansión con el Gobierno de Jair Bolsonaro[7]. En efecto, uno de los objetivos planteados por el Grupo de Innovación, patrocinado por IBM, del Brazil US Business Council (principal organización de lobby empresarial dedicado al fortalecimiento de la relación económica y comercial entre Brasil y EE. UU.), es apoyar la adopción de regulaciones en Brasil que promuevan un enfoque flexible y basado en la innovación para la seguridad cibernética y debates público-privados sobre las mejores prácticas cibernéticas y la amenaza del intercambio de información.[8]

Un dato no menor es que, pese al escándalo de espionaje por parte de la Agencia de Seguridad Nacional estadounidense al Gobierno de Dilma Rousseff (que incluyó el hackeo de computadoras de Petrobras), se haya profundizado la cooperación con EE. UU. en áreas clave, como gobierno electrónico, seguridad cibernética y prevención de delitos cibernéticos.[9] En 2016, mientras avanzaba el proceso de impeachment, el Ministerio de Ciencia, Tecnología e Innovación de Brasil y la Fundación Nacional de Ciencia de EE. UU. firmaron un memorando de cooperación en seguridad cibernética.[10]Luego de consumado el golpe, Michel Temer anunció la contratación de un software creado por Microsoft[11] y, en este marco, la empresa inauguró un Centro de Transparencia en Brasil que permite que los gobiernos tengan acceso a información relacionada con la seguridad cibernética.

## Ciberseguridad y política

El espionaje es una de las estrategias que implica intervención en la política interna de los estados. Pero hay otras estrategias que parecen "indirectas" y que, sin embargo, pueden tener un gran impacto en escenarios políticos, como la ciberseguridad en las elecciones.

Algunas de las últimas campañas electorales han estado marcadas por escándalos que sugerían el uso de datos personales obtenidos, de manera ilícita, en redes sociales para influenciar a los votantes, o la manipulación de estos por la vía de mensajes tipo spam en plataformas de comunicación como WhatsApp. El caso de Cambridge Analytica, aplicado en las elecciones presidenciales estadounidenses y en el referéndum del Brexit británico, sería ejemplo de lo primero,[12] mientras que las elecciones brasileñas que llevaron a Bolsonaro a la Presidencia, serían ejemplo de lo segundo. Pero estos no han sido los únicos casos, pues los intentos de confundir a los votantes o difundir información falsa sobre los candidatos son previos al mundo digital.[13]

Los antecedentes o las potenciales amenazas de repetición de estas prácticas, conectadas con operaciones de guerra psicológica que llegan para manipular a la opinión pública en beneficio de determinados intereses, han hecho saltar las alarmas en analistas, dirigentes políticos e, incluso, al mundo de la seguridad. Este último ve en el problema una oportunidad para ampliar servicios y mercados. Ciertamente, las opciones de negocio en esta área son grandes y en expansión, pues se trata de un mundo -el tecnológico- que se renueva e innova constantemente, como muestra el surgimiento de la tecnología 5G, multiplicando sus posibilidades pero también sus vulnerabilidades. Es un área donde también se trasluce la disputa geopolítica en la carrera entre EE. UU. y China, por ser la vanguardia tecnológica.

## Ciberseguridad y guerra tecnológica

China ha aumentado exponencialmente su inversión en ciencia y tecnología, como lo muestra la política industrial "Hecho en China 2025", que apunta a lograr autonomía en áreas clave de la economía. A esto se suman las joint ventures, con empresas de tecnología de punta extranjera, a cambio de abrir acceso al enorme mercado chino y el crecimiento exponencial en el pedido de patentes.[14]



En EE. UU. los “expertos” declaran la existencia de una crisis en STEM (ciencia tecnología, ingeniería y maquinaria) sin precedentes, que estaría beneficiando el desarrollo tecnológico en otros países a costa del rezago tecnológico en EE. UU.[15] Esto pondría en peligro no solo el “bienestar económico” sino la “seguridad” estadounidense, pues la tecnología 5G[16] “aumentaría la capacidad de espionaje de Beijing sobre gobiernos y empresas occidentales”[17] –le quitaría a Occidente el monopolio que viene detentando en este rubro, como muestra Wikileaks.

En noticias recientes, se advierte que en el mercado de la ciberseguridad a nivel global, China es la que más crecerá en los próximos cinco años, abarcando un mercado de casi 18 mil millones de dólares[18].

## Ciberseguridad y noticias falsas: el costado militar

Visto desde una perspectiva amplia, la ciberseguridad tiene que ver también con la lucha en redes por una información fidedigna, es decir, por detectar y neutralizar lo que ahora se conoce como fake news. En este tema se observa una disputa por el relato sobre qué es verdad y qué no. EE. UU. lleva años tratando de asentar la idea de que la Federación de Rusia está diseminando noticias falsas a través de sus medios de comunicación públicos.



Esta idea aparece en revistas militares especializadas,[19] lo que da cuenta del carácter bélico de la denuncia, pero también en declaraciones oficiales de funcionarios estadounidenses. Por ejemplo, en marzo de 2019, el secretario de Estado de EE. UU., Mike Pompeo, declaraba: “Rusia también ha utilizado los órganos de desinformación auspiciados por el Estado como Russia Today (RT) y Sputnik para distraer la atención del desastre humanitario del régimen de Maduro”.[20] Sin embargo, las continuas acusaciones a RT y Sputnik de difundir noticias falsas, o las denuncias de injerencia rusa en las elecciones estadounidenses,[21] parecen, más bien, una campaña más parecida a lo que EE. UU. denuncia.

La construcción de sentido de la amenaza cibernética está plasmada en los principales documentos estratégicos del Gobierno estadounidense. El primer pilar de la Estrategia de Seguridad Nacional de 2017 plantea que, frente a la amenaza cibernética, es necesario “redoblar los esfuerzos para proteger nuestra infraestructura crítica y redes digitales, puesto que las nuevas tecnologías y los nuevos adversarios generan nuevas vulnerabilidades”. La Estrategia de Defensa Nacional de 2018 postula la necesidad de garantizar el avance tecnológico para la guerra, especialmente en cibernética, lo que incluye la computación avanzada, los análisis de “big data” y la inteligencia artificial.[22]

En reciente testimonio ante el Comité de Servicios Armados del Senado sobre la implementación de la Estrategia de Defensa Nacional en ALC, el comandante del Comando Sur, Craig Faller, afirma que China y Rusia “quieren dar forma a un mundo consistente con sus modelos autoritarios” y “están desdibujando las líneas de lo que constituye una amenaza militar a través de la coerción económica, el robo sistémico de tecnología, las campañas de influencia y la actividad cibernética maliciosa”. Además, llama la atención a la inversión en infraestructura de tecnología informática y cibernética que prepara el escenario en una dimensión militar.[23]

La articulación de la ciberseguridad con enfoque militar es evidente si se observa el perfil de las empresas que se dedican a proveer estos servicios, generalmente vinculadas

también con la inteligencia o la venta de armas. El caso de las empresas israelíes, muy activas en América Latina, como Israel Aerospaces Industries, NSO o Elbit Systems Ltd., entre otras, es sintomático de esta imbricación, así como de la penetración del Estado de Israel en la región a través de este tipo de negocios,[24] con importantes consecuencias para las soberanías nacionales, pues comprometen información sensible. Por otra parte, militarizar las redes sociales, ciberarmamento para combatir los ciberataques o la existencia de una carrera armamentística cibernética, son elementos presentes en los analistas[25] que visualizan a la ciberseguridad como parte de la guerra híbrida actual.

## Reflexiones finales

Como siempre que se tocan temas que conciernen a la seguridad, el riesgo radica en utilizar las potenciales amenazas como excusa para limitar o acabar con derechos. La ciberseguridad no es una excepción y ya empieza a usarse para lograr un mayor control de las poblaciones[26] -supuestamente para evitar que terceros actores hagan un mal uso- sin cuestionar el abuso que determinados gobiernos podrían estar ejerciendo también. En este sentido, la ciberseguridad pone sobre la mesa las contradicciones del sistema en su pretendida lucha por una verdad mediática que no es tal, y la defensa de la libertad de expresión. Pero, también, -y quizás esto sea lo más grave- traza líneas que permiten intuir una sociedad distópica de mayores controles, pero más sutiles, en los que las poblaciones sin acceso a información o tecnología privilegiada serán meras convidadas de piedra a la "fiesta de la democracia", cuando no masas manipulables y manipuladas por quienes tienen el control de datos, soportes e información de manera exclusiva.

En este escenario, América Latina tiene varios problemas: pocos países tienen una estrategia de seguridad nacional cibernética, lo que los expone a eventuales ataques; las empresas que venden servicios de ciberseguridad son, en su mayoría, estadounidenses e israelíes (vinculados a una perspectiva militarizada de seguridad y defensa), y es muy probable que en un futuro inmediato se vean desafiadas por la competencia de China en este rubro (de la mano de la tecnología 5G). Por otro lado, la ciberseguridad es parte de una noción militar de seguridad, entendida como herramienta de guerra. En el México del PRI, se acudió a la ciberseguridad para espionaje de opositores, Wikileaks dio pruebas sobre el espionaje de mandatarios de diversos estados por parte de EE. UU.; el caso venezolano muestra cómo los ataques cibernéticos al sistema eléctrico pueden ser utilizados como un arma más. El control de energía eléctrica, sistema de agua, datos electorales, son tan sólo algunos elementos que quedan vulnerables en un mundo en el que la tecnología avanza y atraviesa aspectos de la vida pública y privada. Es por eso urgente que la ciberseguridad sea una cuestión "pública" y que abra el debate sobre sus objetivos y alcances.

## Referencias


[1]https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

[2]https://www.forbes.com/sites/forbesagencycouncil/2018/07/31/five-measures-latin-america-must-take-to-get-up-to-snuff-on-cybersecurity

[3]http://revistas.unla.edu.ar/software/article/view/775

[4]https://www.forbes.com/sites/kalevleetaru/2019/03/09/could-venezuelas-power-outage-really-be-a-cyber-attack/

[5]https://globalmedia-it.com/fortinet-continua-su-fuerte-impulso-en-america-latina-como-empresa-lider-de-ciberseguridad/

[6]https://www.celag.org/lo-dejo-seguridad-la-visita-netanyahu/

[7]https://www.forbes.com/sites/riskmap/2018/11/27/brazils-new-president-and-the-changing-cyber-risk-landscape/#6067b4d25453

[8]https://www.brazilcouncil.org/task-forces-working-groups/innovation/

[9]http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/10390-comunicado-conjunto-da-presidenta-dilma-rousseff-e-do-presidente-barack-obama-washington-30-de-junho-de-2015

[10]http://www.anpg.org.br/15/04/2016/avanca-cooperacao-entre-brasil-e-estados-unidos-em-seguranca-cibernetica/
[11]https://www.windowsclub.com.br/brasil-troca-linux-microsoft/
[12]https://www.celag.org/cambridge-analytica-el-big-data-y-su-influencia-en-las-elecciones/
[13]https://www.brookings.edu/blog/fixgov/2019/07/11/a-short-history-of-campaign-dirty-tricks-before-twitter-and-facebook/
[14]https://www.wipo.int/pressroom/es/articles/2017/article_0013.html
[15]https://www.forbes.com/sites/arthurherman/2018/09/10/americas-high-tech-stem-crisis/#58bdf5baf0a2
[16] Implica un cambio profundo en tecnologías de la comunicación y la información: permitirá un tiempo de respuesta de la red de un milisegundo y una velocidad de conexión 100 veces más rápida que la actual red 4G, además de un ahorro de energía del 90% respecto a los sistemas actuales. Todo indica que en 2020 esta tecnología llegará a las principales ciudades del mundo y China será la gran exportadora.
[17]https://www.bloomberg.com/news/articles/2019-01-18/the-promise-of-5g-is-the-problem-with-huawei-in-eyes-of-critics?srnd=premium-europe
[18]https://www.chinadailyhk.com/articles/11/75/87/1567994910804.html
[19]https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-94/jfq-94_8-17_Jakubowski.pdf?ver=2019-07-25-162024-817
[20]https://translations.state.gov/2019/03/11/secretario-de-estado-michael-r-pompeo-en-declaraciones-a-la-prensa/
[21]https://www.brookings.edu/blog/fixgov/2019/08/09/foreign-campaign-intervention-may-go-way-beyond-russia-to-china-iran-north-korea-and-saudi-arabia/
[22]https://www.celag.org/america-latina-bajo-amenaza-escenarios-y-operaciones-militares-de-ee-uu-en-la-region/
[23]https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/1901790/southcom-chief-stresses-need-for-partnerships-security-cooperation/
[24]https://www.celag.org/lo-dejo-seguridad-la-visita-netanyahu/
[25]https://dialnet.unirioja.es/servlet/articulo?codigo=3837337
[26]https://www.celag.org/eeuu-ciberseguridad-y-control-total-en-la-disputa-geopolitica/

**Arantxa Tirado** es Dra. en Relaciones Internacionales e Integración Europea (UAB) (España).
**Silvina Romano** es Dra. en Ciencia Política (UNC) (Argentina)
**Tamara Lajtman** es Mg. en Estudios Latinoamericanos (UNAM) (Brasil)
**Aníbal García Fernández** es Máster en Estudios Latinoamericanos (UNAM) (México)



# Espionaje, fragmentación y vigilancia: los dispositivos de la manipulación neoliberal

por Jorge Elbaum

En la última semana la empresa Facebook fue condenada en el Reino Unido a pagar una multa de 500.000 libras esterlinas (643.785 dólares) ante el ente público de control de la privacidad de datos personales [1]. En la misma semana la empresa WhatsApp, propiedad de Mark Zuckerberg desde 2014, demandó a la empresa israelí de vigilancia cibernética NSO Group por espiar en 20 países, entre los cuales se encuentra Argentina.

Los funcionarios de WhatsApp señalaron en su acusación que se trata de actividades de espionaje a 1400 objetivos (teléfonos celulares) detectados hasta la actualidad. Entre los relevados figura la vigilancia de 100 periodistas y decenas de activistas de derechos humanos [2]. En julio último, Facebook fue condenado por el gobierno de Estados Unidos a pagar 5.000 millones de dólares por violar las regulaciones de privacidad de la información.

La imputación se refiere a la entrega de 200 millones de perfiles de sus usuarios a la empresa Cambridge Analytica. Dichos datos fueron utilizados en diversas campañas electorales como el Brexit, el triunfo de Mauricio Macri en 2015 y en 2017 y el éxito de Donald Trump en 2016 [3].

A medida que el hechizo neoliberal empieza a trastabillar en diferentes países, empiezan a divisarse los mecanismos utilizados por los poderes concentrados para manipular y confundir a segmentos específicos de la sociedad. Los tres dispositivos centrales que han sido empleados son:

- El espionaje y vigilancia de referentes políticos, gremiales y/o judiciales con el objetivo de controlarlos, extorsionarlos o paralizarlos.
- La segmentación de grupos sociales operables (capaces de ser influidos), utilizando como insumo para su catalogación la Inteligencia Artificial (IA).
- La multiplicación de operaciones de prensa basadas en datos obtenidos por medios ilícitos (sumados a los recursos provenientes de la IA), destinados a imponer climas sociales, culturales y económicos enfrentados a los intereses mayoritarios.

Los tres procedimientos manejan herramental tecnológico y son complementarios a la construcción política clásica, territorial e identitaria. Se superponen y buscan retroalimentarse conjuntamente. Operan sobre conjuntos sociales poco politizados a partir de la utilización de información clasificada que es intervenida y manipulada para conseguir efectos de resentimiento y odio hacia referentes populares. La multa a Facebook y la demanda a NSO Group exhiben la práctica habitual de los tres dispositivos: la modificación, alteración y configuración de relatos públicos acordes a la imposición de intereses concentrados.

El último 11 de septiembre el juez federal Alejo Ramos Padilla tomo declaración testimonial al empresario israelí Dov Kilinsky, quien aparece en los archivos extraídos de las computadoras de Sebastián D'Alessio como un distribuidor de aparatología de seguridad, vigilancia, seguimiento, encriptación y espionaje [4].

En su declaración Kilinsky acepta ser integrante de la Cámara de Comercio Argentino Israelí, liderada por Mario Montoto, a quien D'Alessio identifica en varios intercambios de WhatsApp como "MM" o "el 1". Admite, además, ser el representante de la empresa madre de NSO Group, la Israel Aerospace Industry, IAI, constituyéndose como su representante en Argentina desde 2013 [5].




## Ciberguerra macrista

El interés de Mauricio Macri por el espionaje ilegal se remonta al caso de las escuchas telefónicas sufridas, entre otros, por familiares de las víctimas de la causa AMIA. Una vez asumida la presidencia en diciembre de 2015, luego de que Macri fuera desvinculado en forma sorpresiva de la imputación por espionaje, la tarea quedó en manos de Patricia Bullrich, que apeló a la colaboración de varios intermediarios con empresas israelíes proveedoras de tecnología de seguridad.

El 24 de julio de 2016 Bullrich declaró que "estamos trabajando con la Dirección de Comunicaciones de la Corte (la ex OJOTA, encargada de las escuchas telefónicas) un establecimiento de protocolos. El otro tema al que nos estamos dedicando fuerte es el de la creación de un protocolo unificado de emergencias. El diputado Waldo Wolff lo está trabajando con expertos de distintos lugares en el mundo, para saber qué hacer y cómo operar para que no se colapsen las comunicaciones y la logística" [6].

Meses después de este reconocimiento (o lapsus) público, el diputado Waldo Wolff acompañó a Tel Aviv a Patricia Bullrich a la cuarta Conferencia de Ciberseguridad, exposición en la que se ofertan y comercializan dispositivos tecnológicos destinados al control del terrorismo y la seguridad pública [7].

Del convite participó también Dov Kilinsky. En esa oportunidad el ministerio de Seguridad adquirió un paquete de ciberseguridad que costó al erario público la suma de 5.200.000 de dólares, cuyo desarrollo bien podría haber sido realizado con recursos propios, provenientes de las tecnologías existentes en el INTI o el CONICET.

El software comprado está orientado –según se informó— a prevenir ataques terroristas. Posee la capacidad de recolectar y procesar datos de redes sociales. El último 24 de diciembre de 2018, horas antes de la celebración de la Nochebuena, el diputado Waldo Wolff dialogó con el misógino locutor Baby Etchecopar en su programa radial El Ángel del Mediodía, en relación al aniversario de la muerte de Alberto Nisman, uno de los temas que más apasiona al ex arquero suplente del club Atlanta.

En el transcurso del reportaje pasó desapercibida una frase del legislador, asiduo asistente a los paneles de debate vespertino de carácter político revisteril. "Yo también -afirmó, eufórico— tengo acceso a carpetas de la vida privada de mucha gente" [8].

## Espionaje en América Latina

En enero de 2015, la Corte Suprema de Panamá difundió el resultado de una investigación sobre espionaje de la que resultó imputado el ex Presidente de ese país, Ricardo Martinelli. La imputación, que supuso el inmediato pedido de extradición de Martinelli –que en 2015 se encontraba residiendo en Estados Unidos— se

basó en la acusación de utilizar una aplicación de vigilancia remota conocida como Pegasus, creada y comercializada por NSO Group. Martinelli fue detenido el 12 de junio de 2017 en Miami.

En el juicio el ex Presidente reconoció que el Estado panameño adquirió, durante su presidencia, soportes de espionaje a dos empresas de ciberdefensa israelíes (NSO y MLM Protection), con la que se realizaron escucha y capturas de pantalla de más de 130 celulares de políticos, empresarios y miembros del Poder Judicial [9].

El 19 de junio de 2017 el New York Times (NYT) reveló que el gobierno mexicano y diferentes empresas privadas de ese país desarrollaron acciones de vigilancia, con la utilización de la aplicación Pegasus, contra periodistas, políticos de la oposición, integrantes de organizaciones no gubernamentales y miembros de la Comisión Interamericana de Derechos Humanos (CIDH) que evaluaban la desaparición de los 43 estudiantes de magisterio de Ayotzinapa. La administración del entonces primer mandatario Enrique Peña Nieto, previa al actual gobierno de Andrés Manuel López Obrador, había adquirido el software espía Pegasus a través de la Procuración de la Nación, el 29 de octubre de 2014, con un costo de 32 millones de dólares.

Según los datos revelados por el NYT, entre los vigilados por el gobierno mexicano se hallaban periodistas como Carmen Aristegui, una de las más reconocidas de ese país. La fuente prioritaria del artículo publicado por el NYT fue el dossier difundido por Citizen Lab, de la Universidad de Toronto, uno de los centros más rigurosos en el monitoreo de las políticas que atentan en todo el mundo contra la privacidad. Su relevamiento se titula “Espionaje gubernamental: monitoreo sistemático de periodistas y defensores de derechos humanos en México” [10].

Pocos días después de esta investigación del NYT, el 17 de septiembre de 2017, Horacio Verbitsky divulgó pormenores de la visita del primer ministro Benjamín Netanyahu a la Argentina, detallando los acuerdos alcanzados con el gobierno de Macri. Entre los integrantes de la numerosa comitiva de empresarios que acompañaron al líder del Likud, partido de la derecha israelí, figuraban los CEOs de dos corporaciones, MLM Protection y NSO Group.[11]

Los funcionarios comercializadores de Pegasus recordaron ante interlocutores del gobierno argentino que NSO fue fundada en 2010 por mayor general Avigdor (Janusz) Ben-Gal, quien fuera anteriormente presidente de la empresa estatal Industrias Aeroespaciales de Israel (IAI). MSO y MLM son dos de las start-ups creadas a partir de la planificación militar estratégica, con base militar de la Unidad 8200, ubicada en el Neguev, cerca de Beersheva, encargada de la investigación y la comercialización de productos ligados a la ciberguerra.

A partir de la asunción de Alberto Fernández y CFK, una parte indeterminada de la información obtenida mediante la utilización de esta aparatología quedará en manos privadas. Por su parte, los dispositivos adquiridos por la actual gestión macrista seguirán controlados en forma remota por quienes los comercializan y los datos obtenidos seguirán almacenados en servidores lejanos, dispuestos a ser utilizados como ariete político en los próximos 4 años.

La ingenuidad es un territorio fértil para el asombro y el descubrimiento en territorios donde prima la honestidad y el mutuo reconocimiento. Pero puede ser una maldición en la gestión política donde los monstruos de las corporaciones trasnacionales se disponen, con minuciosidad planificada, a limarte hasta las ganas de vivir. Habrá que construir mecanismos de respuesta para enfrentar tamaño poder. Hay recursos suficientes para hacerlo. Descuidarse supondría una omisión imperdonable.

## Notas

[1]. La multa es ínfima porque la Ley que pena el robo de la información para su utilización en Inteligencia Artificial (IA) fue aprobada en 2018, y el delito juzgado es anterior a dicha regulación. En la actualidad la misma infracción supondría un monto cercano a los 1000 millones de dólares.

[2]. http://bit.ly/2q41391 y http://bit.ly/2q69cty

[3]. http://bit.ly/2NttTHF

[4]. Ver la excelente cobertura realizada por el periodista Juan Alonso para La Insuperable http://bit.ly/33fccTb y Nuestras Voces, http://bit.ly/322oJaX

[5]. Declaración de Dov Kilinsky ante el juez. Página 7. En: http://bit.ly/324rI2P

[6]. http://bit.ly/336HE5J

[7]. http://bit.ly/2C1DJez

[8]. http://bit.ly/336VGV5. La frase se encuentra en el minuto 7.20.

[9]. http://bit.ly/2C486RI

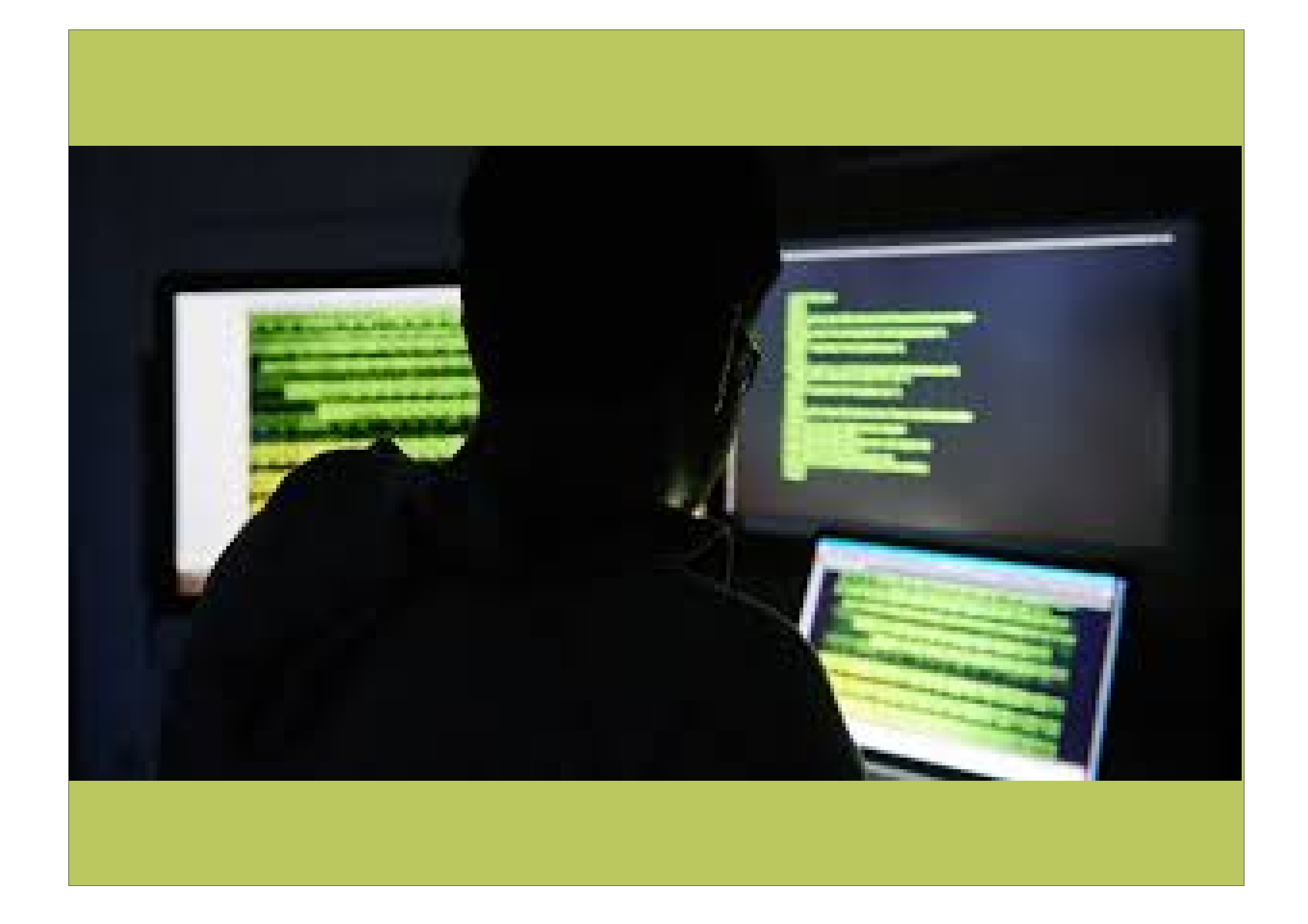
[10]. http://bit.ly/2Nv9FgJ

[11]. A fines de 2014 el fondo de inversión Francisco Partners (FP) adquirió el 70 por ciento del paquete accionario de NSO Group por un monto de 140 millones de dólares. Al momento de la compra tuvo que aceptar los requerimientos de las políticas de seguridad del vendedor, que exige la continuidad operativa de la gestión de este tipo de empresas (y de la ubicación de sus servidores) en Israel. Uno de los más importantes inversores de FP es curiosamente Paul Singer, el máximo referente de los fondos buitres a quien Macri concedió un pago de 10.000 millones de dólares en abril de 2016. Todo cierra.

*Sociólogo, doctor en Ciencias Económicas, analista senior del Centro Latinoamericano de Análisis Estratégico (CLAE, www.estrategia.la). Publicado en elcohetealaluna.com

## Enlace al original:

http://estrategia.la/2019/11/04/espionaje-fragmentacion-y-vigilancia-los-dispositivos-de-la-manipulacion-neoliberal/



# La ciberguerra en la disputa intercapitalista

por Adriana Franco

El ciberespacio se ha configurado como un dominio estratégico tanto para la reproducción del sistema capitalista como para la resistencia. Así, a pesar de que la génesis de este espacio se dio en las entrañas del sujeto hegemónico-Estados Unidos-, ciertos actores y acciones han puesto en riesgo el dominio estadounidense sobre este medio. El hackeo es la principal amenaza en este espacio, debido a que es una actividad que busca eludir la vigilancia del sistema, oponerse a las normas establecidas, quebrantar las estructuras de poder, así como mantener y potenciar la capacidad de actuar en este dominio.

## El control de internet

Internet-que está formado por un conjunto de redes, cables, servidores, sistemas de comunicación, entre otros- es la base material del ciberespacios. A pesar de que este es un medio asequible para quienes tienen los recursos económicos y tecnológicos para incursionar en él, es un campo que está coordinado por un sector privado denominado Internet Corporation for Assigned Names and Numbers (ICANN), el cual favorece a Estados Unidos, ya que "Washington conserva la autoridad de supervisión y su Comité Asesor Gubernamental, compuesto por delegados de otras naciones, no tiene poderes reales" (Cukier, 2005: 7).

Asimismo, en la red de redes hay un dominio de nombres para determinar la ubicación de los servidores, un código para que las máquinas puedan ser reconocidas por las demás, servidores matrices y estándares técnicos que regulan el tráfico de datos (Cukier, 2005: 8-9).

De acuerdo con ICANN, actualmente hay 13 servidores matriz. Diez de estos están controlados por Estados Unidos: cinco por empresas (dos por Verisign, uno por Cogent Communications, otro por ICANN y uno más por Internet System Consortium Inc.), dos por universidades (University of Southern California y University of Maryland) y tres por agencias o departamentos (Departamento de Defensa, Ames Research Center de la NASA y el Laboratorio de Investigación del Ejército). Los demás están regulados por Netnod, Suecia; el Centro de Coordinación de Redes IP europeas, Ámsterdam; y otro por Wide Project, Japón.

## Los ciberataques como reposicionamiento a la asimetría de poder

En el ciberespacio las y los enemigos son los hackers. Un ciberataque implica la generación de un código que daña las estructuras y sistemas computacionales del enemigo.

Para Estados Unidos, el ciberespacio es un medio lleno de incertidumbre que se ha configurado como un dominio de competencia con enemigos altamente calificados. (Nieto 2014: 105). Por esta razón, en 2009, el Departamento de Defensa creó un subcomando conjunto de combate para hacer frente a las amenazas de los hackers: CYBERCOM, el cual está vinculado con la Agencia Nacional de Seguridad (NSA) (Nieto 2014: 98).

El ciberespacio es el quinto dominio de la guerra (Desforges, 2014: 75-76). El general Paul M. Nakasone, comandante del CYBERCOM, considera que su control es fundamental para la hegemonía estadounidense, debido a que en este espacio sus adversarios pueden realizar ataques en contra de sus intereses estratégicosdificultando la posibilidad de una respuesta directa (Nakasone, 2019).

Un ciberataque puede afectar esencialmente tres elementos: las tecnologías de la información, lo cual atentaría contra las capacidades combativas en tierra de las fuerzas armadas; las tecnologías operacionales, que pueden dañar los software y hardware desde los



cuales opera la infraestructura militar y económica del sujeto hegemónico; y las plataformas y sistemas de armas (William, 2018), incluyendo las nucleares. El ejemplo más significativo de un ataque de este tipo se dio en 2010 con Stuxnet, el malware con el que se dañaron las centrifugadoras de Natanz en Irán (Bommakanti, 2018: 3-7).

Este ciberataque fue realizado por la Agencia de Nacional Seguridad (NSA) de EE.UU.y por la Unidad Secreta Israelí 8200. El programa para desarrollar el malware inició en 2007 y su nombre era "OlympicGames" (Gates, 2012). De acuerdo con los análisis de seguridad que se han hecho, el ataque en Natanzentró en el sistema de control industrial de lasinstalaciones infectando computadoras y sistemas en el complejo de enriquecimiento de uranio, lo que generó daños a las centrifugadoras.

Antes de 2010, el Departamento de Defensa estadounidense ya había demostrado la posibilidad de acceder a computadoras que controlaban redes eléctricas con el ejercicio “Eligible Receiver”. Sin embargo, Stuxnet logró superar el air-gapping y entrar a una red cerrada (Porche, Sollinger, McKay, 2011: 1).

Stuxnet es considerada la primera arma digital y a partir de su utilización el ciberespacio se ha convertido en un dominio de suma importancia para la disputa intercapitalista, pero también para los esfuerzos por eliminar el sistema de vigilancia, control y explotación en el que vivimos. De acuerdo con informes de la Corporación de Investigación y Desarrollo (RAND), China y Rusia están destinando cada vez más recursos para la guerra de información con Occidente. Ese mismo reporte considera que a pesar de que estas herramientas y estrategias están en un periodo inicial, ya han generado efectos negativos significativos para la hegemonía estadounidense (Mazarr&Demus, 2019).

## El ciberespacio en la disputa intercapitalista: capacidades y estrategias

La NSA y el CYBERCOM fueron unidos desde el nacimiento del segundo. Sin embargo, en los últimos años, las funciones del CYBERCOM se han vinculado más con el ataque a redes enemigas para alcanzar metas militares y no tanto para desarrollar misiones de espionaje (Greenberg, 2018).

De acuerdo con Nakasone, los principales Estados que ponen en riesgo la ciberseguridad estadounidense son Rusia, China, Irán y Corea del Norte.  Sin embargo, quienes cuentan con mejores capacidades y estrategias son los dos primeros.

El enfoque central del gobierno chino en este ámbito es mantener una presencia significativa para garantizar su seguridad nacional, preservar la estabilidad social y asegurar la información crítica, concentrándose más en el control interno de su población que en algún ataque al exterior (Jinghua, 2019).

No obstante, las capacidades cibernéticas que China está desarrollando podrían reducir las asimetrías en el campo físico de batalla. Asimismo, China tiene la PLA's Unit 61398, que es la oficina central militar de operaciones de red cibernética del gobierno.

China ha sido identificada como una de las principales fuentes de tráfico de ciberataques, empero, esto no significa que desde esta espacio se originen las irrupciones, ya que las y los hackers pueden enrutar el tráfico en otras vías para atribuir la procedencia del ataque a un espacio geográfico diferente (Richards, 2014: 46-48).

Por su parte, Rusia no utiliza el concepto ciberguerra, sino guerra de información, el cual incluye operaciones de redes computacionales, de información, psicológicas, así como la guerra electrónica.

Este gobierno utilizó sus capacidades cibernéticas como una fuerza habilitadora en Georgia y Ucrania (Connell&Vogler, 2016). Asimismo, Rusia tiene una unidad de elite militar que se encarga de llevar a cabo operaciones de espionaje de alto riesgo en el ciberespacio (Oliphant, 2018) y en los últimos años, el gobierno ruso ha estado reclutando programadores con el objetivo de crear un equipo de elite de hackers (Kramer, 2016).

Por esta razón, EE.UU.está desarrollando tecnologías para no permitir que sus adversarios logren sus objetivos en el ciberespacio, por medio de estrategias defensivas y capacitación especializada para oficiales en Fort Gordon (Sheftick, 2019).

Una de las principales preocupaciones de EE.UU.es que gran parte de su infraestructura y economía se basa en la digitalización y autonomización, lo que hace que su régimen sea vulnerable en las dinámicas del ciberespacio.



Durante la administración Trump, se señaló que el CYBERCOM había logrado entrar en las instalaciones eléctricas de Rusia con un malware capaz de interrumpir su red eléctrica. Rusia mencionó que sus sistemas eran inmunes a esos ataques, pero que si Estados Unidos intervenía en su infraestructura esto generaría una guerra cibernética entre ambos Estados (Sanger&Perlroth 2019).

En términos generales, el ciberespacio es un medio que permite reducir asimetrías, como en el caso de China, pero también es un dominio que posibilita la reproducción hegemónica liderada por EE.UU .Actualmente, el país con mejores capacidades en este espacio es EE.UU., sin embargo, Rusia y China están invirtiendo tiempo y dinero para mejorar su competencia en este medio. A pesar de que en las narrativas securitarias estadounidenses, se resalta la amenaza que representa China para la seguridad nacional del país, el Estado con el que ha tenido mayores encuentros en este domino es Rusia.

## El ciberespacio para la creación de mundos alternativos

El ciberespacio no sólo es un dominio ocupado por las grandes potencias, también es un medio en el cual diversos actores sociales tiene capacidad de actuación y movimiento.

Asimismo, no todas las agresiones van dirigidas a infraestructura de redes y comunicaciones, los ciberataquestambién pueden manipular a la población y modificar sus opiniones y decisiones a través de campañas en las cuales se difundan rumores u otras ideas en las redes o medios de comunicación. Entonces, el control del ciberespacio puede garantizar la reproducción hegemónica –a partir de la difusión de los valores e ideas capitalistas– o transformarlas relaciones sociales en las que se sustenta el sistema dominante.

El poder económico y tecnológico de los Estados ha hecho que estos actores sean los ejes centrales en la disputa cibernética, sin embargo, figuras no estatales también han desafiado al sujeto hegemónico a través de la filtración de documentos estratégicos, como lo ejemplifican los casos de Edward Snowden, Julian Assange, Wikileaks y Anonymous. La principal amenaza a la reproducción sistémica no viene de los Estados sino de los individuos o colectivos que han incursionado e irrumpido este espacio a través del hackeo.

"Hackear un sistema requiere conocer sus normas mejor que la gente que lo ha creado o que lo gestiona, y vulnerar la distancia que exista entre el funcionamiento que esa gente haya pretendido darle al sistema y el funcionamiento que muestra el sistema de verdad, o que alguien puede hacer que muestre" (Snowden, 2019: 52).

Así, aunque aún nos hacen falta herramientas y estrategias, el ciberespacio es un dominio que la sociedad puede utilizar para modificar la hegemonía en el ámbito de la reproducción, es decir, la ocupación y apropiación del ciberespacio pueden ayudarnos a romper las relaciones de poder imperante por medio de la inhabilitación de los sistemas que garantizan el predominio de los sujetos que reproducen la hegemonía, de la transmisión de perspectivas de vida diferentes, de la actuación en colectivo y, por lo tanto, de la transformación de las relaciones sociales dominantes para crear un mundo diferente.

**Adriana Franco** es maestra en Estudios de Asia y África, integrante de OLAG y Secretaria Técnica de Investigación del Centro de Relaciones Internacionales de la UNAM.

*Artículo publicado en la revista América Latina en Movimiento de ALAI, No. 544, octubre 2019, "Las redes de la guerra" (co-edición con OLAG).*

## Fuentes consultadas


Bommakanti, K.2018 “The Impact of Cyber Warfare on Nuclear Deterrence: A Conceptual and Empirical Overview”, ORF Issue Brief 266: 1-15.

Connell, M. &Vogler, S. 2016 Russia's Approach to Cyber Warfare, CNA Analysis & Solutions.

Cukier, K. N. 2005 "Who Will Control the Internet? Washington Battles theWorld", Foreign Affairs 84, 6: 7-13.

Greenberg, A. 2018 "The Next NSA Chief Is More Used to Cyberwar Than Spy Games" The Wired.

Hérodote 2014 Cyberspace: en jeux géopolitiques,no. 152-153, primer y segundo trimestre.

Jinghua, L. 2019 "What Are China's Cyber Capabilities and Intentions?" Carnegie Endowment for International Peace.

The New York Times:Kramer, Andre E.2016 "How Russia Recruited Elite Hackers for Its Cyberwar" / Sanger, David E. &Perlroth Nicole (2019) "U.S. Escalates Online Attacks on Russia's Power Grid".

RAND Corporation: Porche, I.R., Sollinger, J. M., McKay, S.2011 A Cyberworm that Knows No Boundaries / Mazarr&Demus 2019 “Hostile Social Manipulation by Russia and China a Growing but Poorly Understood Threat”.

Nakasone, P. M. 2019 “A Cyber Force for Persistent Operations" Joint Force Quarterly 92: 10-14.

Oliphant, R. 2018 "What is the Unit 26165, Russia's elite military hacking centre?" The Telegraph.

Richards, J. 2014 Cyber-War: The Anatomy of the Global Security Threat, Palgrave Macmillan.
Sheftick, Gary 2019 "Cyber Teams Safeguard National Security" U.S.Department of Defense.
Snowden, Edward. 2019 Vigilancia permanente, Planeta.